

<b>Notice of Allowability</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/549,396	ROHATGI, PANKAI	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- **The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1.  This communication is responsive to 6/30/2004.
2.  The allowed claim(s) is/are 1-31,33 and 35-44.
3.  The drawings filed on \_\_\_\_\_ are accepted by the Examiner.
4.  Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a)  All    b)  Some\*    c)  None    of the:
    1.  Certified copies of the priority documents have been received.
    2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
6.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
  - (a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
    - 1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_\_.
  - (b)  including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
7.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

#### Attachment(s)

1.  Notice of References Cited (PTO-892)
2.  Notice of Draftsperson's Patent Drawing Review (PTO-948)
3.  Information Disclosure Statements (PTO-1449 or PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4.  Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5.  Notice of Informal Patent Application (PTO-152)
6.  Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_.
7.  Examiner's Amendment/Comment
8.  Examiner's Statement of Reasons for Allowance
9.  Other \_\_\_\_\_.

*E. Moise*  
**EMMANUEL L. MOISE**  
**PRIMARY EXAMINER**  
*AUG 21/36*

**DETAILED ACTION**  
**EXAMINER'S AMENDMENT**

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Louis P. Herzberg on 8/4/2004.

Cancel new claims 45,46 and 47 on pages 11-12 of the CLAIM AMENDMENTS AND LISTING filed on 6/30/2004.

**Examiner's Statement of Reasons for Allowance**

Claims *1-31, 33, 35-44* are allowed over prior art.

By amending claims 1, 10, 23, 29, 31 and 35 , the Applicant has overcome the rejection based 35 USC 101.

The Examiner acknowledges the terminal disclaimer filed on Feb. 5, 2004 to obviate a double patenting rejection over prior Patent (6,701,434) which was mailed on 11/05/2003.

The following is an examiner's statement of reasons for the indication of allowable claimed subject matter.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of

Reasons for Allowance.”

**As per claim 1,** Prior art of record , US Pat. 4,309,509 directed to Ralph C. Merkle discusses converting a one time scheme into an N time scheme so called Basic Merkle Scheme, whereby n key pairs ( $PK_j, SK_j$ ) for n one-time scheme is generated. Then, using a secure hash function , pre-hashed values of the one-time public keys are computed to get the Merkle root r of authentication tree. The public key r is outputted and the n pairs ( $PK_j, SK_j$ ) and the Merkle tree are stored as the secret key.

Although Merkle’s public key ( r) reads on a public key which includes commitment (that is hash of  $Pk_j$  and its sibling) . Merkle basic scheme fails to teach a *private key which includes at least one enhancing key*, see A Certified Digital Signature, Advances in Cryptology, Crypto ’89, LNCS 435, pp 218-238,1990.

**As per claims 10, 29,** Prior art of record directed to M. Belare , P. Rogaway, Collision-Resistant Hashing: Towards making UOWHFs Practical teaches a signing with an TCR Hash family where the signing algorithm chooses K ,anew for each message (i.e. a first string). Belare further teaches that the key K is included with the signature. That is a second TCR function is applied to a second string that includes key K, see pages 26-27, see also page 28. Belare discloses the steps of verifying a message using TCR function for verifying the TCR commitment message generated , see page 26.

Belare et al fail to teach a TCR commitment which hides “ *all information about the value that is committed*”. That is Belare’s message in the signature is a public knowledge.

**As per claims 23, 31 and 35,** Prior art of record, Leighton et al (5,432,852) discusses Lamport digital signature scheme by converting a hash function into a 1-time signature scheme(col. 2, lines 45-63).

Leighton further discloses the main drawback of the 1-time schemes as being used to sign a single message. To overcome this disadvantage , it is also known in the art how to convert a 1-time scheme into an N-time scheme. One technique for converting a one time scheme into an N time scheme is the so called Basic Merkle Scheme , A Certified Digital Signature, Advances in Cryptology, Crypto '89, LNCS 435, pp 218-238,1990) whereby n key pairs ( $PK_j, SK_j$ ) for then n one-time scheme is generated. Then, using a secure hash function , pre-hashed values of the one-time public keys are computed to get the Merkle root r of authentication tree. The public key r is outputted and the n pairs ( $PK_j, SK_j$ ) and the Merkle tree are stored as the secret key.

*Leighton's hash function is not a TCR function . Therefore, the resulting digital signature is not a TCR commitment message . That is, in a digital signature scheme, the message (M) that is signed is public knowledge , whereas the TCR commitment (as recited in claims 23, 31 and 35), has to hide all information about the value that is committed by using a TCR commitment function.*

Prior art of record singly or in combination does not teach or fairly suggest a commitment based digital signature using a private key which includes an enhancing key in a public/private key pair in such a way that the enhancing key is also hidden in the corresponding public key as a commitment to the enhancing key. By defining enhancing keys as TCR keys , both message and the key are authenticated and verified providing fast and compact commitment based digital signature.

Dependent claims 2-9,11-22, 24-28, 30, 33, 36-44 are also allowed by virtue of their dependencies.

***Conclusion***

Any inquiry concerning this communication or earlier communications from examiner should be directed to Taghi Arani, whose telephone number is (703) 305-4274. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned is:

(703) 872-9306

Taghi Arani  
Patent Examiner  
8/4/2004

*E. Moise*  
EMMANUEL L. MOISE  
PRIMARY EXAMINER  
*A/W 2136*